

CLAIM AMENDMENTS

Claim Amendment Summary

Claims pending

- Before this Amendment: Claims 1-27 and 29-36.
- After this Amendment: Claims 1-3, 5-7, 10, 14-22, 24-26, 29, and 31-32.

Non-Elected, Canceled, or Withdrawn claims: Claims 4, 8-9, 11-13, 23, 27-28, 30, and 33-36.

Amended claims: Claims 1, 5-7, 10, 14-22, 24-26, 29, and 31-32.

New claims: None.

Claims:

1. (Currently Amended) A computer-readable medium having computer-executable instructions for securing data that, when executed by a computer, performs acts comprising:

obtaining two input polynomials each with degree 5, wherein a first polynomial is nominally described as $a(X) = a_0 + a_1X + a_2X^2 + a_3X^3 + a_4X^4 + a_5X^5$ and a second polynomial is nominally described as $b(X) = b_0 + b_1X + b_2X^2 + b_3X^3 + b_4X^4 + b_5X^5$ and terms a_5 and b_5 are non-zero values;

computing a product polynomial of the input polynomials, wherein the total number of coefficient multiplication operations is fewer than or equal to seventeen, wherein during the computing, calculating:

$$\begin{aligned}
 & (a_0 + a_1 + a_2 + a_3 + a_4 + a_5)(b_0 + b_1 + b_2 + b_3 + b_4 + b_5)C \\
 & + (a_1 + a_2 + a_3 + a_4 + a_5)(b_1 + b_2 + b_3 + b_4 + b_5)(-C + X^6) \\
 & + (a_0 + a_1 + a_2 + a_4)(b_0 + b_1 + b_3 + b_4)(-C + X^4) \\
 & + (a_0 - a_2 - a_3 + a_5)(b_0 - b_2 - b_3 + b_5)(C - X^7 + X^6 - X^5 + X^4 - \\
 & X^3) \\
 & + (a_0 - a_2 - a_5)(b_0 - b_2 - b_5)(C - X^5 + X^4 - X^3) \\
 & + (a_0 + a_3 - a_5)(b_0 + b_3 - b_5)(C - X^7 + X^6 - X^5) \\
 & + (a_0 + a_1 + a_2)(b_1 + b_1 + b_2)(C - X^7 + X^6 - 2X^5 + 2X^4 - 2X^3 + X \\
 & 2) \\
 & + (a_2 + a_4 + a_5)(b_3 + b_4 + b_5)(C + X^8 - 2X^7 + 2X^6 - 2X^5 + X^4 - X \\
 & 3) \\
 & + (a_2 + a_3)(b_2 + b_3)(-2C + X^7 - X^6 + 2X^5 - X^4 + X^3) \\
 & + (a_1 - a_4)(b_1 - b_4)(-C + X^4 - X^5 + X^6) \\
 & + (a_1 + a_2)(b_1 + b_2)(-C + X^7 - 2X^6 + 2X^5 - 2X^4 + 3X^3 - X^2) \\
 & + (a_2 + a_4)(b_2 + b_4)(-C - X^8 + 3X^7 - 2X^6 + 2X^5 - 2X^4 + X^3) \\
 & + (a_0 + a_1)(b_0 + b_1)(-C + X^7 - X^6 + 2X^5 - 3X^4 + 2X^3 - X^2 + X) \\
 & + (a_4 + a_5)(b_4 + b_5)(-C + X^9 - X^8 + 2X^7 - 3X^6 + 2X^5 - X^4 + X^3) \\
 & + a_0 b_1(-3C + 2X^7 - 2X^6 + 3X^5 - 2X^4 + 2X^3 - X + 1) \\
 & + a_1 b_1(3C - X^7 - X^5 + X^4 - 3X^3 + 2X^2 - X) \\
 & + a_4 b_4(3C - X^9 + 2X^8 - 3X^7 + X^6 - X^5 - X^3) \\
 & + a_5 b_5(-3C + X^{10} - X^9 + 2X^7 - 2X^6 + 3X^5 - 2X^4 + 2X^3)
 \end{aligned}$$

to compute the product polynomial;
reporting results of the computing, whereby the computed results facilitate
data security.

2. (Original) A medium as recited in claim 1 further comprising repeating the obtaining and the computing.

3. (Original) A medium as recited in claim 1 further comprising:
selecting a pair of polynomials from a collection of pairs and providing the selected polynomials to the obtaining;
repeating the selecting, obtaining, and computing.

4. (Canceled)

5. (Currently Amended) A medium as recited in claim [4] 1, wherein the variable X is replaced by its negative ($-X$) and the odd-indexed coefficients, a_1, a_3, b_1, b_3, b_5 , are replaced by their negatives.

6. (Currently Amended) A medium as recited in claim [4] 1, wherein the computing is performed in a finite field of characteristic 2, with each even coefficient replaced by zero and each odd coefficient replaced by one.

7. **(Currently Amended)** A medium as recited in claim [4] 1, wherein the computing is performed in a finite field of characteristic 3, with each coefficient in claim 4 replaced by its modulo 3 image 0, 1 or -1.

8. **(Canceled)**

9. **(Canceled)**

10. **(Currently Amended)** A computing device for securing data comprising:

an audio/visual output ;

a computer-readable medium having computer-executable instructions that, when executed by a computer, performs acts comprising:

obtaining two input polynomials each with degree $[\leq] 5$, wherein a first polynomial is nominally described as $a(X) = a_0 + a_1X + a_2X^2 + a_3X^3 + a_4X^4 + a_5X^5$ and a second polynomial is nominally described as $b(X) = b_0 + b_1X + b_2X^2 + b_3X^3 + b_4X^4 + b_5X^5$ and terms a_5 and b_5 are non-zero values;

computing a product polynomial of the input polynomials, wherein the total number of coefficient multiplication operations is fewer than or equal to seventeen, wherein during the computing, calculating:

$$\begin{aligned}
& (a_0 + a_1 + a_2 + a_3 + a_4 + a_5)(b_0 + b_1 + b_2 + b_3 + b_4 + b_5) C \\
& + (a_1 + a_2 + a_3 + a_4)(b_1 + b_2 + b_3 + b_4)(-C + X^6) \\
& + (a_0 + a_1 + a_3 + a_4)(b_0 + b_1 + b_3 + b_4)(-C + X^4) \\
& + (a_0 - a_2 - a_3 + a_5)(b_0 - b_2 - b_3 + b_5)(C - X^7 + X^6 - X^5 + X^4 - \\
& X^3) \\
& + (a_0 - a_2 - a_5)(b_0 - b_2 - b_5)(C - X^5 + X^4 - X^3) \\
& + (a_0 + a_3 - a_5)(b_0 + b_3 - b_5)(C - X^7 + X^6 - X^5) \\
& + (a_0 + a_1 + a_2)(b_0 + b_1 + b_2)(C - X^7 + X^6 - 2X^5 + 2X^4 - 2X^3 + X \\
& 2) \\
& + (a_3 + a_4 + a_5)(b_3 + b_4 + b_5)(C + X^8 - 2X^7 + 2X^6 - 2X^5 + X^4 - X \\
& 3) \\
& + (a_2 + a_3)(b_2 + b_3)(-2C + X^7 - X^6 + 2X^5 - X^4 + X^3) \\
& + (a_1 - a_4)(b_1 - b_4)(-C + X^4 - X^5 + X^6) \\
& + (a_1 + a_2)(b_1 + b_2)(-C + X^7 - 2X^6 + 2X^5 - 2X^4 + 3X^3 - X^2) \\
& + (a_3 + a_4)(b_3 + b_4)(-C - X^8 + 3X^7 - 2X^6 + 2X^5 - 2X^4 + X^3) \\
& + (a_0 + a_1)(b_0 + b_1)(-C + X^7 - X^6 + 2X^5 - 3X^4 + 2X^3 - X^2 + X) \\
& + (a_4 + a_5)(b_4 + b_5)(-C + X^9 - X^8 + 2X^7 - 3X^6 + 2X^5 - X^4 + X^3) \\
& + a_0 b_0 (-3C + 2X^7 - 2X^6 + 3X^5 - 2X^4 + 2X^3 - X + 1) \\
& + a_1 b_1 (3C - X^7 - X^5 + X^4 - 3X^3 + 2X^2 - X) \\
& + a_4 b_4 (3C - X^9 + 2X^8 - 3X^7 + X^6 - X^5 - X^3) \\
& + a_5 b_5 (-3C + X^{10} - X^9 + 2X^8 - 2X^7 + 3X^6 - 2X^4 + 2X^3)
\end{aligned}$$

to compute the product polynomial;

reporting results of the computing, whereby the computed results facilitate data security.

11. (Canceled)

12. (Canceled)

13. (Canceled)

14. (Currently Amended) A medium as recited in claim [11] 1, wherein the computing is performed in a finite field of characteristic 3, with each coefficient in claim 4 replaced by its modulo 3 image 0, 1 or -1.

15. (Currently Amended) A medium as recited in claim [11] 1 further comprising repeating the obtaining and the computing.

16. (Currently Amended) A medium as recited in claim [11] 1 further comprising:

selecting a pair of polynomials from a collection of one or more pairs of polynomials and providing the selected polynomials to the obtaining;

repeating the selecting, obtaining, and computing.

17. (Currently Amended) A medium as recited in claim [11] 1, wherein the total number of coefficient multiplication operations performed during the computing is fewer than or equal to seventeen.

18. (Currently Amended) A medium as recited in claim ~~[11]~~ 1, wherein the two input polynomials are representative of integers base R and a length n and wherein $X = R$ in the calculating.

19. (Currently Amended) A medium as recited in claim ~~[11]~~ 1, wherein C is zero.

20. (Currently Amended) A computer-implemented method for securing data comprising:

obtaining two input polynomials with six terms each, wherein a first polynomial is nominally described as $a(X) = a_0 + a_1X + a_2X^2 + a_3X^3 + a_4X^4 + a_5X^5$ and a second polynomial is nominally described as $b(X) = b_0 + b_1X + b_2X^2 + b_3X^3 + b_4X^4 + b_5X^5$ and terms a_5 and b_5 are non-zero values;

computing a product polynomial of the input polynomials, wherein the total number of coefficient multiplication operations is fewer than or equal to seventeen, wherein during the computing, calculating:

$$\begin{aligned}
 & \underline{(a_0 + a_1 + a_2 + a_3 + a_4 + a_5)(b_0 + b_1 + b_2 + b_3 + b_4 + b_5)C} \\
 & \underline{+ (a_1 + a_2 + a_3 + a_4)(b_1 + b_2 + b_3 + b_4)(-C + X^6)} \\
 & \underline{+ (a_0 + a_1 + a_2 + a_3)(b_0 + b_1 + b_2 + b_3)(-C + X^4)} \\
 & \underline{+ (a_0 - a_2 - a_3 + a_5)(b_0 - b_2 - b_3 + b_5)(C - X^7 + X^6 - X^5 + X^4 -} \\
 & \underline{X^3)} \\
 & \underline{+ (a_0 - a_2 - a_5)(b_0 - b_2 - b_5)(C - X^5 + X^4 - X^3)} \\
 & \underline{+ (a_0 + a_3 - a_5)(b_0 + b_3 - b_5)(C - X^7 + X^6 - X^5)} \\
 & \underline{+ (a_0 + a_1 + a_2)(b_0 + b_1 + b_2)(C - X^7 + X^6 - 2X^5 + 2X^4 - 2X^3 + X} \\
 & \underline{2)} \\
 & \underline{+ (a_3 + a_4 + a_5)(b_3 + b_4 + b_5)(C + X^8 - 2X^7 + 2X^6 - 2X^5 + X^4 - X} \\
 & \underline{3)} \\
 & \underline{+ (a_2 + a_3)(b_2 + b_3)(-2C + X^7 - X^6 + 2X^5 - X^4 + X^3)} \\
 & \underline{+ (a_1 - a_4)(b_1 - b_4)(-C + X^4 - X^5 + X^6)} \\
 & \underline{+ (a_1 + a_2)(b_1 + b_2)(-C + X^7 - 2X^6 + 2X^5 - 2X^4 + 3X^3 - X^2)} \\
 & \underline{+ (a_3 + a_4)(b_3 + b_4)(-C - X^8 + 3X^7 - 2X^6 + 2X^5 - 2X^4 + X^3)}
 \end{aligned}$$

$$\begin{aligned}
& + (a_0 + a_1)(b_0 + b_1)(-C + X^7 - X^6 + 2X^5 - 3X^4 + 2X^3 - X^2 + X) \\
& + (a_1 + a_2)(b_1 + b_2)(-C + X^9 - X^8 + 2X^7 - 3X^6 + 2X^5 - X^4 + X^3) \\
& + a_0 b_0 (-3C + 2X^7 - 2X^6 + 3X^5 - 2X^4 + 2X^3 - X + 1) \\
& + a_1 b_1 (3C - X^7 - X^5 + X^4 - 3X^3 + 2X^2 - X) \\
& + a_1 b_1 (3C - X^9 + 2X^8 - 3X^7 + X^6 - X^5 - X^3) \\
& + a_2 b_2 (-3C + X^{10} - X^9 + 2X^7 - 2X^6 + 3X^5 - 2X^4 + 2X^3)
\end{aligned}$$

to compute the product polynomial;

reporting results of the computing, whereby the computed results facilitate data security.

21. (Currently Amended) A computer-implemented method as recited in claim 20 further comprising repeating the obtaining and the computing.

22. (Currently Amended) A computer-implemented method as recited in claim 20 further comprising:

selecting a pair of polynomials from a collection of one or more pairs of polynomials and providing the selected polynomials to the obtaining;

repeating the selecting, obtaining, and computing.

23. (Canceled)

24. (Currently Amended) A computer-implemented method as recited in claim [23] 20, wherein the variable X is replaced by its negative ($-X$) and the odd-indexed coefficients, a_1 , a_3 , a_5 , b_1 , b_3 , b_5 , are replaced by their negatives.

25. (Currently Amended) A computer-implemented method as recited in claim [23] 20, wherein the computing is performed in a finite field of characteristic 2, with each even coefficient replaced by zero and each odd coefficient replaced by one.

26. (Currently Amended) A computer-implemented method as recited in claim [23] 20, wherein the computing is performed in a finite field of characteristic 3, with each coefficient in claim 4 replaced by its modulo 3 image 0, 1 or -1 .

27. (Canceled)

28. (Canceled)

29. (Currently Amended) A system facilitating cryptographic security, the system comprising:

a memory comprising a set of computer program instructions; and
a processor coupled to the memory, the processor being configured to execute the computer program instructions, which comprise:

obtaining two input polynomials with six terms each, wherein a first polynomial is nominally described as $a(X) = a_0 + a_1X + a_2X^2 + a_3X^3 + a_4X^4 + a_5X^5$ and a second polynomial is nominally described as $b(X) = b_0 + b_1X + b_2X^2 + b_3X^3 + b_4X^4 + b_5X^5$ and terms a_5 and b_5 are non-zero values;

computing a product polynomial of the input polynomials, wherein the total number of coefficient multiplication operations is fewer than or equal to seventeen, wherein during the computing, calculating:

$$\begin{aligned}
& \underline{(a_0 + a_1 + a_2 + a_3 + a_4 + a_5)(b_0 + b_1 + b_2 + b_3 + b_4 + b_5)C} \\
& \underline{+ (a_1 + a_2 + a_3 + a_5)(b_1 + b_2 + b_4 + b_5)(-C + X^6)} \\
& \underline{+ (a_0 + a_1 + a_3 + a_4)(b_0 + b_1 + b_3 + b_4)(-C + X^4)} \\
& \underline{+ (a_0 - a_2 - a_3 + a_5)(b_0 - b_2 - b_3 + b_5)(C - X^7 + X^6 - X^5 + X^4 - X^3)} \\
& \underline{+ (a_0 - a_2 - a_5)(b_0 - b_2 - b_5)(C - X^5 + X^4 - X^3)} \\
& \underline{+ (a_0 + a_3 - a_5)(b_0 + b_3 - b_5)(C - X^7 + X^6 - X^5)} \\
& \underline{+ (a_0 + a_1 + a_2)(b_0 + b_1 + b_2)(C - X^7 + X^6 - 2X^5 + 2X^4 - 2X^3 + X^2)} \\
& \underline{+ (a_3 + a_4 + a_5)(b_3 + b_4 + b_5)(C + X^8 - 2X^7 + 2X^6 - 2X^5 + X^4 - X^3)} \\
& \underline{+ (a_2 + a_3)(b_2 + b_3)(-2C + X^7 - X^6 + 2X^5 - X^4 + X^3)} \\
& \underline{+ (a_1 - a_4)(b_1 - b_4)(-C + X^4 - X^5 + X^6)} \\
& \underline{+ (a_1 + a_2)(b_1 + b_2)(-C + X^7 - 2X^6 + 2X^5 - 2X^4 + 3X^3 - X^2)} \\
& \underline{+ (a_3 + a_4)(b_3 + b_4)(-C - X^8 + 3X^7 - 2X^6 + 2X^5 - 2X^4 + X^3)} \\
& \underline{+ (a_0 + a_1)(b_0 + b_1)(-C + X^7 - X^6 + 2X^5 - 3X^4 + 2X^3 - X^2 + X)} \\
& \underline{+ (a_4 + a_5)(b_4 + b_5)(-C + X^9 - X^8 + 2X^7 - 3X^6 + 2X^5 - X^4 + X^3)} \\
& \underline{+ a_0 b_0 (-3C + 2X^7 - 2X^6 + 3X^5 - 2X^4 + 2X^3 - X + 1)} \\
& \underline{+ a_1 b_1 (3C - X^7 - X^5 + X^4 - 3X^3 + 2X^2 - X)} \\
& \underline{+ a_4 b_4 (3C - X^9 + 2X^8 - 3X^7 + X^6 - X^5 - X^3)} \\
& \underline{+ a_5 b_5 (-3C + X^{10} - X^9 + 2X^8 - 2X^7 + 3X^6 - 2X^4 + 2X^3)}
\end{aligned}$$

to compute the product polynomial;

reporting results of the computing, whereby the computed results
facilitate data security.

30. (Canceled)

31. (Currently Amended) A system as recited in claim [30] 29, wherein the variable X is replaced by its negative ($-X$) and the odd-indexed coefficients, $a_1, a_3, a_5, b_1, b_3, b_5$, are replaced by their negatives.

32. (Currently Amended) A system as recited in claim [30] 29, wherein the computing is performed in a finite field of characteristic 2, with each even coefficient replaced by zero and each odd coefficient replaced by one.

33. (Canceled)

34. (Canceled)

35. (Canceled)

36. (Canceled)